AMENDMENTS

In the Claims

Please delete Claims 16-18, 21-24, 29-30, 32-33 and 37-39 without prejudice, and amend the remaining claims as follows:

1. – 9. (canceled)

10. (currently amended) A method for secure communication between a client and a server in a data processing system, the method comprising:

generating a client message at the client;

retrieving an embedded server public key from a read-only memory structure in an article of manufacture in the client, the read-only memory structure having an embedded client private key, the embedded server public key and the embedded client private key not being related by a public/private key pair relationship, the embedded client private key being associated with a client public key generated and stored exclusively outside the client;

encrypting the client message with the embedded server public key;

sending the client message to the server;

receiving a server message including application code from the server at the client in response to the client message, the application code having a first portion encrypted with a server private key and a second portion, wherein the first portion of the application code is small relative to the second portion of the application code; ~~and~~

authenticating the first portion of the application code with the embedded server public key; and

authenticating the second portion of the application code using an integrity checking algorithm that is not a public key algorithm.

11. (previously presented) The method of claim 10 further comprising:

retrieving client authentication data;

retrieving an embedded client private key from a read-only memory structure in an article of manufacture in the client;

encrypting the client authentication data with the embedded client private key; and

storing the encrypted client authentication data in the client message.

12. (original) The method of claim 11 further comprising:

retrieving an embedded client serial number from a read-only memory structure in an article of manufacture in the client; and

storing a copy of the embedded client serial number in the client message.

13. – 18. (canceled)

19. (currently amended) A method for secure communication between a client and a server in a data processing system, the method comprising:

generating a first server message at the server, the first server message including application code ~~having a first portion~~ encrypted with a server private key and ~~a second portion, the first portion being~~ authenticable with a server public key, wherein the application code includes a program that performs a download using symmetric keys;

retrieving information that was requested by the client;

storing the retrieved information in ~~the~~ a second server message encrypted with the symmetric keys;

~~retrieving a client public key, wherein the client public key corresponds to an embedded client private key in a read-only memory structure in an article of manufacture in the client, and the client public key is generated and stored exclusively outside the client;~~

~~encrypting the server message with the client public key; and~~

sending the first server message to the client;

authenticating the first server message at the client using the server public key; and

executing the program at the client to download the second server message from the server.

20. (previously presented) The method of claim 19 further comprising:

retrieving server authentication data;

retrieving the server private key;

encrypting the server authentication data with the server private key; and

storing the encrypted server authentication data in the server message.

21. – 24. (canceled)

25. (currently amended) A method for secure communication between a client and a server in a data processing system, the method comprising:

receiving a client message from the client;

retrieving a server private key;

decrypting the client message with the server private key;

retrieving a client serial number from the decrypted client message;

retrieving a client public key that is associatively stored with the retrieved client serial number, wherein the client public key corresponds to an embedded client private key in a read-only memory structure in an article of manufacture in the client and is generated and stored exclusively outside the client; and

generating a server message including application code at the server in response to the client message, the application code having a first portion encrypted with the server private key and a second portion, the first portion being authenticable with a server public key and the second portion being authenticable with an integrity checking algorithm that is not a public key algorithm, wherein the first portion of the application code is small relative to the second portion of the application code;

wherein the read-only memory structure has an embedded server public key, the embedded server public key and the embedded client private key not being related by a public/private key pair relationship.

26. (original) The method of claim 25 further comprising:

retrieving encrypted client authentication data from the client message;

decrypting the client authentication data with the retrieved client public key; and

verifying the decrypted client authentication data.

27. – 30. (canceled)

31. (currently amended) A method for secure communication between a client and a server in a data processing system, the method comprising:

receiving a first server message from the server at the client, the first server message including first application code ~~having a first portion~~ encrypted with a server private key ~~and a second portion~~, wherein the first application code includes a program that performs a download using symmetric keys;

~~retrieving an embedded client private key from a read-only memory structure in an article of manufacture in the client, the embedded client private key being associated with a client public key generated and stored exclusively outside the client;~~

~~decrypting the server message with the embedded client private key; and~~

authenticating the first ~~portion of the~~ application code with a server public key; and

executing the program at the client to download a second server message from the server, the second server message including second application code requested by the client, wherein the first application code is small relative to the second application code.

32. – 39. (canceled)